IN THE CLAIMS

The following listing of the claims replaces all previous listings:

1. (Currently Amended) A user authentication apparatus for authenticating a user by verification of biometrics which are presented by the user and are a biological characteristic unique to the individual user, comprising:

~~authentication means for authenticating a user by verification of biometrics of the user which is a biological characteristic unique to an individual;~~

acquisition means operable when the authentication by ~~said authentication means~~ the verification of the biometrics results in failure, ~~in the verification of the biometrics~~ for acquiring biometrics data of the user who has requested ~~for~~ the authentication using a sensor and converting the acquired biometrics data into digital data; and

storage means for storing the digital data obtained by the conversion by said acquisition means; and

substitute authentication means for substituting the verification of biometrics when the biometrics data is acquired by said acquisition means and performing substitute authentication based on data other than the data acquired by said acquisition means.

2. (Currently Amended) A user authentication apparatus as claimed in claim 1, further comprising ~~storage~~

means for discriminating whether or not biometrics data inputted so as to be used for the verification of biometrics have a quality suitable for automatic verification, and means operable when it is discriminated that the biometrics data do not have an image quality sufficient

for characteristic extraction in the verification of biometrics for storing the digital data obtained by the conversion by said acquisition means ~~storing the biometrics data acquired by said acquisition means, and processing means for performing search and pursuit of an illegal user based on the biometrics data stored in said storage means.~~

3. (Currently Amended) A user authentication apparatus as claimed in claim 2~~1~~, further comprising means

operable when it is discriminated that the biometrics data do not have an image quality sufficient for the characteristic extraction for discriminating whether or not the biometrics data are legal biometrics data of the biological characteristic, and wherein, ~~inputted so as to be used for the verification of biometrics have a quality suitable for automatic verification, and means operable~~ when it is discriminated that the biometrics data ~~do not have a quality suitable for automatic comparison for storing the acquired~~ are the legal biometrics data~~.~~ of the biological characteristic, use of said substitute authentication means is permitted.

4. (Currently Amended) A user authentication apparatus as claimed in claim 3, ~~further comprising means~~ wherein the discrimination of whether or not the biometrics data are the legal biometrics data depends upon discrimination of whether or not the inputted biometrics data are proper and inputted by the user at the place.

~~operable when it is discriminated that the biometrics data do not have a quality suitable for automatic comparison for discriminating whether or not the biometrics data have a quality suitable for use for the search and the pursuit of an illegal user, and wherein, when it is~~

~~discriminated that the biometrics data are suitable for use for the search and the pursuit of an illegal user, use of said substitute authentication means is permitted.~~

5. (Currently Amended) A user authentication apparatus as claimed in claim 4, wherein a correlation of a plurality of ~~the discrimination of whether or not the~~ biometrics data acquired using said sensor is measured to perform ~~are suitable for use for the search and the pursuit of an illegal user depends upon~~ discrimination of whether or not the ~~inputted~~ biometrics data are ~~proper and~~ inputted by the user at the place.

a1

6. (Currently Amended) A user authentication apparatus as claimed in claim 1~~5~~, wherein at least a fingerprint is used as the biometrics. ~~a correlation of a plurality of biometrics data acquired by said acquisition means is measured to perform discrimination of whether or not the biometrics data are inputted by the user at the place.~~

7. (Currently Amended) A user authentication apparatus as claimed in claim 1, wherein, upon the storage of the ~~at least a fingerprint is used as the~~ biometrics~~.~~ data acquired using said sensor, at least an image of an inputting process of a fingerprint is photographed and stored.

8. (Original) A user authentication apparatus as claimed in claim 1, wherein, upon storage of biometrics data prior to the substitute authentication, at least an image of the face and/or

a figure when a fingerprint is inputted are photographed.

9. (Currently Amended) A user authentication method, comprising the steps of:

authenticating a user by verification of biometrics which is a biological characteristic unique to an individual;

acquiring, when the authentication results in failure in the verification of the biometrics, biometrics data of a user who has requested for the authentication and storing the biometrics data; and

performing substitution authentication based on data other than the biometrics data for substituting the verification of biometrics when the biometrics data are acquired by said acquisition means.

A1

10. (Original) A user authentication method as claimed in claim 9, further comprising a step of storing the biometrics data acquired by the step of acquiring the biometrics data, and search and pursuit of an illegal user are performed based on the stored biometrics data.

11. (Original) A user authentication method as claimed in claim 9, further comprising a step of discriminating whether or not biometrics data inputted so as to be used for the verification of biometrics have a quality suitable for automatic verification, and a step of storing the acquired biometrics data when it is discriminated that the biometrics data do not have a quality suitable for automatic comparison.

12. (Original) A user authentication method as claimed in claim 11, further comprising a step of discriminating, when it is discriminated that the biometrics data do not have a quality suitable for automatic comparison, whether or not the biometrics data have a quality

suitable for use for the search and the pursuit of an illegal user, and wherein, when it is discriminated that the biometrics data are suitable for use for the search and the pursuit of an illegal user, use of the substitute authentication is permitted.

13. (Original) A user authentication method as claimed in claim 12, wherein the discrimination of whether or not the biometrics data are suitable for use for the search and the pursuit of an illegal user depends upon discrimination of whether or not the inputted biometrics data are proper and inputted by the user at the place is used.

a1 cancel

14. (Original) A user authentication method as claimed in claim 13, wherein a correlation of a plurality of biometrics data acquired by the step of acquiring the biometrics data is measured to perform discrimination of whether or not the biometrics data are inputted by the user at the place.

15. (Original) A user authentication method as claimed in claim 9, wherein at least a fingerprint is used as the biometrics.

16. (Original) A user authentication method as claimed in claim 9, wherein, upon storage of biometrics data prior to the substitute authentication, at least an image of the face and/or a figure when a fingerprint is inputted are photographed.